REMARKS

Claim Rejections

Claims 1-8 stand rejected under 35 U.S.C. 112 as failing to comply with the written description requirement.

Claims 16-20 stand rejected under 35 U.S.C. 112 as indefinite.

Claims 1-4, 8 and 16-19 stand rejected under 35 USC 103(a) as unpatentable over U.S. Patent Publication No. 2002/0071557 (Nguyen) in view of Federal Information Processing Standards Publication 186 (FIPS).

Claims 5-7 and 20 stand rejected under 35 USC 103(a) as unpatentable over Nguyen in view of FIPS and further in view of U.S. Patent No. 5,885,158 (Torango et al.).

Claims 9-15 and 21-23 stand rejected under 35 U.S.C. 103(a) as unpatentable over Torango et al. in view of Nguyen and FIPS.

Claim Amendments

The claims have been amended to eliminate the rejections under 35 U.S.C. 112 and to patentably distinguish over the cited references.

The Cited Art

Nguyen discloses a gaming system in which gaming machines securely communicate with devices over a public network such as the Internet. (Abstract). The gaming system includes methods for providing gaming licenses, data acquisition and other gaming transactions. (¶0015). The system includes a method of sharing transaction data between a gaming machine and a remote server. The transaction data is encrypted and sent to the remote server. The transaction data includes accounting data, game usage data, game configuration data, software version data, etc. (¶0016). The system also provides for sending a game license request message from a gaming machine to a remote server. A game license reply message from the remote server includes a game license, updating the license data on the gaming machine. (¶0017). The system further provides for sending a gaming report request message from a gaming machine to a remote server, receiving a gaming report reply message from the remote server and when the gaming report reply message includes a gaming report, displaying the gaming report on a gaming machine. (¶0019). The remote server may also generate a reply message indicating that an original message from a gaming machine was received. The reply message may include the

requested information. For instance, the remote server may request diagnostic data or a report of some type from the gaming machine. The data in the reply message may be encrypted. (¶0062).

FIPS discloses signature generation and verification techniques using a secure hash algorithum.

Torango et al. discloses a progressive gaming system. A win event can be automatically generated by a win of a progressive game event at a gaming terminal. (Col. 15, lines 41-51). A cluster controller determines whether the identity of a gaming terminal is valid. (Col. 16, lines 1-15).

Applicants' Claimed Invention Would Not Have Been Obvious

The cited references neither disclose not suggest Applicants' claimed methods, as set out in amended independent claims 1, 9, 16, and 21. Additionally, the cited references do not disclose the two-message procedure of claims 7, 14, and 19 or the single, signed message procedure of claims 8 and 15.

Nguyen discloses a system for proving network security between a gaming machine and a remote server. Nguyen's system does not use a hashing function to digitally sign and verify a bonus or other type of command. Additionally, Nguyen does not disclose a system in which a bonus or other command originates at a master server. Rather, in Nguyen's system, messages are originated at the gaming machines.

Nguyen also does not disclose performing an action in response to a command if a digitally signed command at a receiving node matches a digitally signed command from a transmitting node. Instead, in Nguyen, messages are simply encrypted and decrypted for security purposes. Any action performed is not predicated on verifying or authenticating the validity of the received message.

Further, Nguyen does not disclose providing a digitally signed command including a session key that is changeable and associated with a session index so that a receiving node can determine the session key used. This feature of Applicants' claimed invention further enhances security. See Applicants' specification page 9, line 5 to page 11, line 10.

Additionally, Nguyen does not disclose raising an alarm or issuing a notice if a digitally signed command at a receiving node does not match a digitally signed command from the transmitting node. This provides an additional safeguard and also improves system security. (See Applicants' specification, page 15, lines 25-28).

FIPS and Torango et al. do not cure these deficiencies of Nguyen. FIPS merely discloses techniques using a secure harsh algorithum, and Torango et al. discloses a progressive gaming

system in which the identity of a gaming machine is validated as part of the prize award process.

The combination of references do not disclose, for example, as called for by amended claim 1, generating a command at a master server or slave server, digitally signing the command by performing a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digitally signed command including a session key that is changeable and associated with a session index so that a receiving node can determine the session key used, transmitting a digitally signed command from a transmitting node at the master server or slave server to a receiving node, and performing an action in response to the command only if the digitally signed command at the receiving node matches the digitally signed command from the transmitting node and if the digitally signed command at the receiving node does not match the digitally signed command from the transmitting node, issuing an alarm or a notice.

Therefore, Applicants' claimed invention would not have been obvious in view of Nguyen, Torango et al or FIPS.

Conclusion

In view of the foregoing, it is respectfully submitted that all the claims are now in condition for allowance. Accordingly, allowance of the claims at the earliest possible date is requested.

If prosecution of this application can be assisted by telephone, the Examiner is requested to call Applicants' undersigned attorney at (510) 663-1100.

If any fees are due in connection with the filing of this amendment (including any fees due for an extension of time), such fees may be charged to Deposit Account No. 504480 (Order No. IGT1P306X1).

Dated: October 21, 2008

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/William J. Egan, III/

William J. Egan, III
Reg. No. 28,411

P.O. Box 70250
Oakland, CA 94612-025030